

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

**STIPULATION OF
EXPECTED TESTIMONY**

SA Alfred Williamson

17 June 2013

It is hereby agreed by the Accused, Defense Counsel, and Trial Counsel, that if SA Alfred Williamson were present to testify during the merits and pre-sentencing phases of this court-martial, he would testify substantially as follows:

1. I began working for the Computer Crimes Investigation Unit (CCIU) of the U.S. Army Criminal Investigation Command (CID) in 2006. I am currently a criminal investigator Special Agent (SA). In 2010 and 2011, I was a digital forensic examiner and SA, working in the Digital Forensics and Research Branch of CCIU. SA David Shaver was my supervisor. Prior to working for CCIU, I worked as a computer forensic Special Agent for the Department of Homeland Security from 2002 to 2006. From 1992 to 2002, I served as a police officer in Texas.
2. I have attended and received training in multiple areas related computer forensic examination. This training includes Treasury Department computer forensic courses through the Federal Law Enforcement Training Center, nine weeks of intermittent training in A Plus, pre-computer evidence response, and basic computer evidence response techniques. For my work with CIIU, I have attended additional training on digital media collection and forensic examination, as well as computer crime scene investigation, from the Defense Cyber Investigations Training Academy (DCITA), under the Defense Cyber Crime Center (DC3). I have industry certifications from CompTIA in A Plus, Network Plus, and Security Plus. Further, I am a Microsoft certified specialist in Windows Vista and a certified Ethical Hacker. I have obtained all three Department of Defense forensic examination certifications in digital media collection, digital examination, and computer crimes investigations. I am also a certified EnCase Examiner through Guidance Software, the makers of the EnCase forensic tool. Finally, I have GIAC certifications in forensic examination and analysis, as well as security.
3. As part of this case, I conducted a forensic examination of **Prosecution Exhibit (PE) 11**, a U.S. government NIPRNET computer collected from the supply annex on FOB Hammer, Iraq. The IP address of this computer was 144.107.17.19. Specifically, I examined the verified-by-hash forensic image obtained by SA Calder Robertson from the hard drive of this computer. The original forensic laboratory examination request came from one of the CID agents in Iraq, SA Toni Graham. Initial examination of the forensic image revealed that it contained the Windows XP operating system and the computer was set to Baghdad time (GMT +3:00). Before beginning my examination of the forensic image, I performed a standard virus scan on this computer and confirmed that it had no malicious files.

143 / 02

4. I used the EnCase forensic software tool to conduct my examination. This software is commonly used by forensic examiners. It verifies the hash value of the evidence being examined so that the examiner can be sure he is analyzing an exact duplicate of the originally collected evidence. A hash value is a unique identifier for a piece of electronic information that is made up of a series of numbers and letters. I have used EnCase software extensively. I encountered no errors during my examination. Overall, my forensic examination identified four main things of note. I will address each finding in turn.

5. The supply annex NIPRNET computer was not configured for Common Access Card (CAC) login, as the "scforceoption" value was not present. Instead, a username and password were required to logon. On login to the computer by a user, the computer was set to display a Department of Defense warning banner and legal notice. The notice read:

****ATTENTION!**** This is a DOD computer system. Before processing classified information, check the security accreditation level of this system. Do not process, store, or transmit information classified above the accreditation level of this system. This computer system, including all related equipment, networks and network devices (includes Internet access) are provided only for authorized U.S. Government use. DOD computer systems may be monitored for all lawful purposes, including ensuring that use authorized, for management of the system, to facilitate protection against unauthorized access and to verify security procedures, survivability, and operational security. Monitoring includes, but is not limited to, active attacks by authorized DOD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DOD computer system, authorized or unauthorized, constitutes consent to monitoring. Unauthorized use of this DOD computer system may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. ****Use of this system constitutes consent to monitoring for all lawful purposes.****

The DoD warning banner and legal notice did not explicitly prohibit the downloading of email addresses. I am not aware of any restriction or guidance that precludes one from downloading email addresses from Outlook.

6. The supply annex NIPRNET computer had a "bradley.manning" user account. This account was not created until 21 May 2010. My examination revealed that the user of the bradley.manning user account visited the website <http://news.google.com> and searched for "wikileaks" on 21 May 2010. The bradley.manning user account visited websites related to non-judicial punishment under Article 15 on 21 May 2010. The bradley.manning user account also visited several websites owned by Google in order to gain access to a Gmail email account, also

on 21 May 2010. I also looked at the Microsoft Outlook nickname file under the bradley.manning user account. The nickname list or file is automatically generated when a user sends an email with Microsoft Outlook. This nickname file revealed two email addresses associated with Mr. Adrian Lamo. When I examined the Recycle Bin of the bradley.manning user account, I found a text file that contained the contents of a PGP-encrypted email communication between PFC Manning and Mr. Adrian Lamo. The text file was named "Second Attempt". This "Second Attempt" text file was initially located under "My Documents", but was later moved by the user to the Recycle Bin.

7. Other than the items just described, I initially found very little of investigative interest under the bradley.manning user account. I later went back and examined the entire computer, including the other user accounts present on the computer, when Mr. Mark Johnson found references to the United States Forces-Iraq Global Address List (GAL) during his examination of PFC Manning's personal computer, including extracts of what appeared to be a Microsoft Exchange GAL with thousands of email addresses. Accordingly, I went back and examined the entire computer, including the "peter.bigelow" user account.

8. When I looked at the supply annex NIPRNET again, it appeared to me that PFC Manning or someone with access to his personal accounts was operating the computer under the user account peter.bigelow. I say this for several reasons.

9. First, examination of the "My Documents" folder under the peter.bigelow user account revealed a large text file that appeared to be an extract of a Microsoft Exchange GAL. The text file was named "blah.txt". "Blah" is a naming convention that was used by PFC Manning for files on his personal computer and his SIPRNET computer.

10. Second, I found five files related to the GAL in the Recycle Bin of the peter.bigelow user account—two text files named "blah.txt", two ".zip" archives named "blah.zip" (each containing a text file named "blah.txt"), and a text file named "tmp.txt". All of these files found in the Recycle Bin appeared to have been created and deleted on 13 May 2010, and in between creating and deleting these files, the user of the peter.bigelow account also viewed the bradley.e.manning Gmail account inbox. All of these files, text files and .zip archives, contained extracts of what appeared to be a Microsoft Exchange GAL similar to the content of the text file found under the "My Documents" folder. I was not surprised to find various files, because given the huge amount of data a Global Address List contains, it would be easier to manage fragments rather than a whole intact file.

11. As stated before, I found two large text files named "blah.txt" contained within the ".zip" archives in the Recycle Bin of the peter.bigelow user account. The two text files are different. One contains approximately 74,000 Exchange-formatted email addresses (emails text file), and the other contains the units, ranks, and sections of personnel that correspond with the email addresses (names text file). **PE 47 for ID** is a CD containing the names text file. If fully printed, this text file would be 1,386 pages. **PE 47 for ID** is a twenty-page excerpt from the names text file. **PE 48 for ID** is a CD containing the emails text file. If fully printed, this text file would also be 1,386 pages. **PE 48 for ID** is a twenty-page excerpt from the emails text file. I did not contact any individual who could have given me the actual Iraq GAL, nor did I compare

the data in the files recovered from the above files with the actual Iraq GAL. I did not attempt to communicate with any of the email addresses located in the above files and am unaware whether the listed emails were functioning.

12. Third, someone using the peter.bigelow account also searched for “wikileaks” and “julian assange”.

13. Fourth, the Recycle Bin of the peter.bigelow user account contained a PDF of military documents pertaining to PFC Manning named “tmp.pdf”.

14. Finally, the Internet history for the peter.bigelow user account contained web pages displaying the logged-in user as PFC Manning. Specifically, in the “index.dat” file, I observed logins to PFC Manning’s Army Knowledge Online (AKO) email account, as well as logins to the bradley.e.manning Gmail account. “Index.dat” is a file used by Windows to record website and local files accessed by a user to help speed up the loading of pages in Microsoft Internet Explorer and Windows Explorer. I also found several temporary internet files that were Amazon.com webpages. One of the pages displayed PFC Manning’s name and address in the “Shipping to” and “Billing” sections. There was no evidence in the “index.dat” file that a user of the peter.bigelow account visited the Twitter or WikiLeaks websites, nor did I find any evidence that the user visited anti-American or extremist websites. My forensic examinations produced no evidence of a Wikileaks Most Wanted list or any suspicious financial transactions. I found no references to Jason Katz during my investigation.

15. With regards to the Global Address List information, I also found evidence that the user of the peter.bigelow user account had searched for information on the internet relating to the global address list. Specifically, in the temporary internet files, I found a Google search page with results for searching “global address list Microsoft excel macro”. This search occurred on 11 May 2010. A Microsoft Excel macro is a computer program used within Microsoft Excel to automate common procedures within Microsoft Excel. **PE 44 for ID** is a printout of the search page from this computer showing the Google results that I was able to recover from the computer in the temporary internet files. **PE 45 for ID** is a search page showing Google results for a search for “global address list macro outlook”. This search also occurred on 11 May 2010 and this webpage was recovered from the temporary internet files as well. A Microsoft Outlook Macro is similar to the description above for a Microsoft Excel Macro, but for Microsoft Office. **PE 46 for ID** is a Google search page with results from a search for “vba outlook write text file”. This search occurred on 13 May 2010. “VBA” is short for “Visual Basic for Applications.” This Google search provided links to instructions on how to computer program in Visual Basic, a common programming language for Microsoft Office products, that can be used to export information from Outlook to a “.txt” file, although emails can also be saved by clicking on “save as” in Outlook and selecting “.txt” file type. Temporary internet files is a folder in the Windows operating system used to cache or store websites visited by the user through Internet Explorer or other web browsers. The storing or caching of these webpages allows these websites to load more quickly the next time they are visited by the user. They are also used typically by forensic examiners to determine what webpages a user previously accessed.

Jodean Morrow
JODEAN MORROW
CPT, JA
Assistant Trial Counsel

Thomas F. Hurley
THOMAS HURLEY
MAJ, JA
Defense Counsel

Bradley E. Manning
BRADLEY E. MANNING
PFC, USA
Accused